UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,137	06/30/2003	Shawn E. Wiederin	COS02007	3010

25537 7590 08/06/2007

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
08/06/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

Office Action Summary	Application No.	Applicant(s)	
	10/608,137	WIEDERIN ET AL.	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10,12-16 and 19-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-10,12-16 and 19-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 11 May 2007 amends claims 1, 4, 5, 7-10, 12-14, 16, 19, 20, and 22. Claims 2, 3, 11, 17, 18, and 23-28 have been cancelled. Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant's argument that Suuronen does not disclose "forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious content" has been considered and is persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Schneier, U.S. Publication No. 2002/0087882.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 4, 5, 8-10, 12-14, 16, 19, 20 are rejected under 35 U.S.C. 102(a) and/or 102(e) as being anticipated by Schneier, U.S. Publication No. 2002/0087882. Referring to claim 1, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]),

which meets the limitation of at least one interface configured to receive data transmitted via a network, a firewall configured to; receive data from the at least one interface, determine whether the data potentially contains malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data in the received data that potentially contains malicious content, intrusion detection logic configured to: receive the first data. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, and forwarding logic configured to: receive the report information, forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed, which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content.

Referring to claim 4, Schneier discloses that information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of a virtual private network gateway configured to establish a secure connection with the remote central management system.

Referring to claim 5, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using a signature-based technique.

Referring to claims 8, 9, Schneier discloses that the firewall receives filter updates from the SOC ([0037]), which meets the limitation of the firewall is configured to receive updated rule-based processing information from an external device via the network.

Referring to claim 10, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receiving data transmitted via the network, identifying first data that may contain malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]). The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generating report information based on the first data, forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make

a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed, which meets the limitation of forwarding the first data to the user device when it is determined that the first data does not contain malicious content.

Referring to claim 12, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establishing a virtual private network connection to the external device, and wherein the forwarding the report information includes forwarding the report information over the virtual private network connection.

Referring to claim 13, Schneier discloses that the SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of receiving, from the external device, information indicating whether the first data is to be forwarded to the user device, and dropping the first data when the information indicates that the first data is not to be forwarded.

Referring to claim 14, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of examining the received data for viruses using a signature-based technique.

Referring to claim 16, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receive data transmitted via a network, determine whether the data may contain malicious content using a first set of rules. The firewall receives filter updates from the SOC ([0037]), which meets the limitation of receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data that may contain malicious content based on the determining. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, forward the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the processor. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly

engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed, which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content.

Referring to claim 19, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establish a virtual private network tunnel with the external device and send the report information over the virtual private network tunnel.

Referring to claim 20, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of when identifying first data that may contain malicious content, the instructions cause the processor to identify a virus using a signature-based technique.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 6, 15, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier. U.S. Publication No. 2002/0087882, in view of Judge, U.S. Patent No. 6,941,467. Referring to claims 6, 15, 21, Schneier does not specify that the firewall filters for spam. However. it would have been obvious to one of ordinary skill in the art at the time the invention was made to for the client-side firewall of Schneier to filter for spam because spam consumes resources that negatively impacts productivity as taught by Judge (Col. 4, lines 42-46).

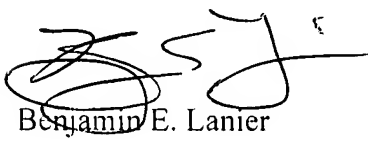
8. Claims 7, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Bates, U.S. Patent No. 6,785,732. Referring to claims 7, 22, Schneier does not specify the type of data traffic that is received by the client-side. Bates discloses virus checking downloaded music files (Col. 10, lines 29-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made for virus-checking functionality in scan all types of data traffic, including downloaded music files, because computer viruses have emerged as a very real threat to data in today's computer systems, and checking files before they are downloaded would help to prevent virus infection as taught by Bates (Col. 1, lines 42-62).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier